II. General Remarks Concerning This Response

Claims 1-40 are currently pending. Claims 1, 5, 7, 10, 12-14, 18, 20, 23, 25-27, 31, 33, 36, and 38-40 have been amended; no claims have been added or canceled. Reconsideration of the claims is requested.

The previous Office action did not indicate if the formal drawings that were filed with the Office on 01/18/2002 were acceptable. Applicant requests that the next Office communication indicates whether the drawings are acceptable.

III. 35 U.S.C. § 102(e)–Anticipation–*Ramasubramani et al.*

The Office action has rejected claims 1-7, 9, and 11-13 under 35 U.S.C. § 102(e) as anticipated by Ramasubramani et al., "Centralized certificate management system for two-way interactive communication devices in data networks", U.S. Patent Number 6,233,577 B1, filed 02/17/1998, issued 05/15/2001. This rejection is traversed.

Ramasubramani et al. discloses the use of digital certificates, but the rejection applies various portions of Ramasubramani et al. against the claims in a manner that is not logical. For example, the rejection argues that the second element of independent claim 1, i.e. "obtaining a host identity for the client from the digital certificate", is disclosed in that "Ramasubramani teaches that digital certificates contain [the] digital signature of the certificate issuer (Column 3 Line 57)." Hence, the rejection appears to argue that the host identity is equivalent to a digital signature. Although Applicant disagrees with this argument, the issue at this point is that the rejection inexplicably argues that the digital signature is equivalent to very different elements in the claim language. The rejection later argues that at least a portion of

the third and fourth elements of claim 1, i.e. "retrieving host-encrypted secret data associated with the host identity from the digital certificate;" and "decrypting the host-encrypted secret data with a host private key", is disclosed in that "Ramasubramani further states that more importantly it contains the digital signature of the certificate issuer, i.e. encrypted 'fingerprint' that can be used to verify the contents of the certificate (Column 3 Line 54)." In other words, it appears that the rejection argues that the digital signature on the digital certificate is equivalent to the host identity and the host-encrypted secret data. This is more illogical given that the claim states that the host-encrypted secret data is decrypted using the host private key; if the digital signature is equivalent to the host-encrypted secret data, it would be generated by using the host private key and then decrypted (verified) using the host public key.

Moreover, because the argument in the rejection makes an analogy between the host-encrypted secret data and the digital signature, the argument is only supportable when the host is the certifying/certificate authority because only the certificate authority should have access to the private key that can decrypt the digital signature from the digital certificate. In contrast, the present invention is directed to authenticating a client that presents the digital certificate to many different classes of host systems that do not include the certificate authority.

Amendments have been made to the claims to clarify the claim language. Given the argument by the rejection, the rejection appears to imply that "the host identity" in the second element of claim 1 refers to the identity of the host, i.e. the identity of the certificate authority in Ramasubramani et al., e.g., similar to an issuer name that might be found in a digital

certificate. The second element of claim 1, as amended, reads: "obtaining a host identity for the client from the digital certificate, wherein the host identity for the client identifies the client to the host, and wherein the host is not a certifying authority that issued the digital certificate". Given the amendment to the claim, an argument cannot be made that the host identity somehow refers to the host because the host identity identifies the client and not the host. Moreover, the claim explicity states that the host is not the certificate/certifying authority that issued the digital certificate.

The third and fourth elements of claim 1 have been amended to change the term "host-encrypted secret data" to "host-decryptable secret data". (Dependent claims 5, 7, and 10, which depend from independent claim 1, have been amended likewise, including to change the term "CA-encrypted secret data" to "CA-decryptable secret data".) Support for this amendment can be found in the specification on page 16, last paragraph, which states that the host's public key is used to encrypt the data. In other words, the term "host-encrypted secret data" was meant to convey the meaning that the secret data was encrypted with the host's public key, but the term may have been misinterpreted in the rejection such that the term was given the meaning that the secret data had been encrypted by the host. Applicant has amended the claim language to use the term "host-decryptable secret data" to convey the meaning that the encrypted secret data can only be decrypted by the host, which is congruent with the fact that the secret data was encrypted using the public key of the host; since only the host should have access to the host's corresponding private key, the encrypted secret data should only be decryptable by the host, thereby making the encrypted secret data equivalent to "host-decryptable secret data".

The Office action uses an anticipation argument against independent claim 12 that is similar to the argument that is used against independent claim 1. Applicant's argument above with respect to the host identity is also applicable to independent claim 12 because it contains language that recites the host identity within the request for the digital certificate.

With respect to the dependent claims, Ramasubramani et al. does not disclose, at a minimum, the subject matter in the independent claims from which these dependent claims depend. Thus, Ramasubramani et al. also fails to disclose the features of the dependent claims because these dependent claims include the features of independent claims. Moreover, the dependent claims, as amended, recite additional elements concerning the use of host-decryptable secret data and CA-decryptable secret data, and these elements also fail to be disclosed in Ramasubramani et al.. For example, dependent claim 10 recites that the host identity and the host-decryptable secret data is contained in an X.509 extension within a digital certificate. This and other features are also clearly absent from Ramasubramani et al., notwithstanding the argument in the rejection.

Ramasubramani et al. clearly does not disclose features as required by the claim language. As stated at MPEP § 2131: "A claim is anticipated only if each and every element as set forth in the claim is found, either expressly or inherently described, in a single prior art reference." *Verdegaal Bros. v. Union Oil Co. of California*, 814 F.2d 628, 631, 2 USPQ2d 1051, 1053 (Fed. Cir. 1987). "The identical invention must be shown in as complete detail as is contained in the ... claim." *Richardson v. Suzuki Motor Co.*, 868 F.2d 1226, 1236, 9 USPQ2d 1913, 1920 (Fed. Cir. 1989). Hence, Ramasubramani et al. cannot be used as an anticipatory reference, and the rejection of claims 1-7, 9, and

11-13 has been overcome, whereby Applicant requests the withdrawal of the rejection.

IV. 35 U.S.C. § 102(e)–Anticipation–*Andrews et al.*

The Office action has rejected claim 40 under 35 U.S.C. § 102(e) as anticipated by Andrews et al., "Risk management for public key management infrastructure using digital certificates", U.S. Patent Number 6,324,645 B1, filed 11/27/2001, issued 08/11/1998. This rejection is traversed.

The novelty of independent claim 40 centers on the last element of the claim, which stated in its original form that "the extension comprises a host identity and host-encrypted secret data associated with the host identity". However, Applicant cannot adequately restate or paraphrase an argument for the rejection when the argument is non-existent in the Office action. The only mention of the host identity within the rejection of independent claim 40 is the last line of the rejection, which states: "Examiner concludes that the extensions contain the host identity." Merely stating that a reference discloses a claimed feature without being able to cite a portion of the reference that teaches the claimed feature is not an adequate anticipation argument.

Since the argument in the rejection with respect to the host identity is so brief, one can only surmise that the argument is intended to rely on Andrews et al. in a manner somewhat similar to the argument that was provided in the rejection of claim 1 based on Ramasubramani et al.. In any case, independent claim 40 has been amended to include language similar to the language that was used in amended independent claim 1. Independent claim 40, as amended, includes the following element:

an extension, wherein the extension comprises a host identity and host-decryptable secret data associated with the host identity, wherein the host identity identifies a client to a host, wherein the host is not a certifying authority that issued the digital certificate, and wherein the host-decryptable secret data is used by the host to authenticate the client.

Andrews et al. simply does not disclose this element.

Andrews et al. clearly does not disclose at least one claimed element. As stated at MPEP § 2131: "A claim is anticipated only if each and every element as set forth in the claim is found, either expressly or inherently described, in a single prior art reference." *Verdegaal Bros. v. Union Oil Co. of California*, 814 F.2d 628, 631, 2 USPQ2d 1051, 1053 (Fed. Cir. 1987). "The identical invention must be shown in as complete detail as is contained in the ... claim." *Richardson v. Suzuki Motor Co.*, 868 F.2d 1226, 1236, 9 USPQ2d 1913, 1920 (Fed. Cir. 1989). Hence, Andrews et al. cannot be used as an anticipatory reference, and the rejection of claim 40 has been overcome, whereby Applicant requests the withdrawal of the rejection.

V. 35 U.S.C. § 103(a)—Obviousness

The Office action has rejected claims 8 and 10 under 35 U.S.C. § 103(a) as being unpatentable over Ramasubramani et al. and Andrews et al.. This rejection is traversed.

Dependent claim 8 reads as follows:

The method of claim 1 wherein the digital certificate comprises multiple host identities for multiple hosts within the distributed data processing system.

Dependent claim 10, as amended, reads as follows:

The method of claim 9 wherein the host identity and the host-decryptable secret data associated with the host identity is stored within an X.509 extension within the digital certificate.

Again, the novelty of these claims centers on the inclusion of a host identity within a digital certificate. In the case of claim 8, the novelty concerns the inclusion of multiple host identities within a digital certificate. In the case of claim 10, the novelty centers on the inclusion of a host identity and its associated host-decryptable secret data within an X.509 extension within the digital certificate. As argued above, neither Ramasubramani et al. nor Andrews et al. disclose the inclusion of a host identity within a digital certificate as claimed. Thus, it is not possible for a rejection to argue that either of these references disclose any teachings regarding a host identity in a digital certificate as claimed; in other words, neither reference can be used as a primary reference or a secondary reference for features that are combinable in a hypothetical system that renders the claimed features obvious.

The examiner bears the burden of establishing a *prima facie* case of obviousness based on the prior art when rejecting claims under 35 U.S.C. § 103. *In re Fritch*, 972 F.2d 1260, 23 U.S.P.Q.2d 1780 (Fed. Cir. 1992). Only when a *prima facie* case of obviousness is established does the burden shift to the applicant to produce evidence of nonobviousness. *In re Oetiker*, 977 F.2d 1443, 1445, 24 U.S.P.Q.2d 1443, 1444 (Fed. Cir. 1992); *In re Rijckaert*, 9 F.3d 1531, 1532, 28 U.S.P.Q.2d 1955, 1956 (Fed. Cir. 1993). If the Patent Office does not produce a *prima facie* case of unpatentability, then without more the applicant is entitled to the grant of a patent. *In re Oetiker*, 977 F.2d 1443, 1445, 24 U.S.P.Q.2d 1443, 1444 (Fed. Cir. 1992); *In re Grabiak*, 769 F.2d 729, 733, 226 U.S.P.Q. 870, 873 (Fed. Cir. 1985). In response to an assertion of obviousness by the Patent Office, the applicant may attack the Patent Office's *prima facie* determination as improperly made out, present objective evidence tending

to support a conclusion of nonobviousness, or both. *In re Fritch*, 972 F.2d 1260, 1265, 23 U.S.P.Q.2d 1780, 1783 (Fed. Cir. 1992).

With respect to claims 8 and 10, the rejection does not point out the necessary teachings, suggestions, or incentives to reach the claimed invention. Hence, the rejection of the claims does not establish a *prima facie* case of obviousness based on the prior art. Therefore, the rejection of the claims under 35 U.S.C. § 103(a) has been shown to be insupportable, and these claims are patentable over the applied prior art. Applicant requests the withdrawal of the rejection.

With respect to the remaining claims, the Office action does not state which grounds of rejection are used to reject each claim; the Office action merely relies on the previous rejections and states that the remaining claims are rejected under similar rationales. Applicant asserts that the arguments that Applicant has provided above are also applicable to the other claims.

VI. Conclusion

It is respectfully urged that the present application is patentable, and Applicant kindly requests a Notice of Allowance.

For any other outstanding matters or issues, the examiner is urged to call or fax the below-listed telephone numbers to expedite the prosecution and examination of this application.

DATE: June 1, 2004

Respectfully submitted,

Joseph R. Burwell
Reg. No. 44,468
ATTORNEY FOR APPLICANT

Law Office of Joseph R. Burwell
P.O. Box 28022
Austin, Texas 78755
Voice: 866-728-3688 (866-PATENT8)
Fax: 866-728-3680 (866-PATENT0)
Email: joe@burwell.biz